NATIONAL SECURITY LETTERS

(U//FOUO) National Security letters are an investigative tool that allows the FBI to obtain certain types of information without court intervention:

1. Under the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709, the FBI can obtain telephone and e-mail communication records from telephone companies and internet service providers.
2. Under the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3414(a)(5)(A), the FBI can obtain financial records from financial institutions.
3. Under the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681u(a) and (b), the FBI can obtain a list of financial institutions at which an individual has accounts, as well as consumer identifying information from credit reporting companies.
4. Under the Fair Credit Reporting Act, 15 U.S.C. § 1681v, the FBI can obtain a full credit report in an international terrorism case from credit reporting companies.

(U//FOUO) FCRA causes some confusion because it allows the FBI to obtain different types of information that are not interchangeable. In either a counterterrorism case or a counterintelligence case, the FBI may only obtain through an NSL the financial institutions that the customer maintains or has maintained an account; the customer's name, current and former addresses; and current and former places of employment. 15 U.S.C. § 1681u. A full credit report can be obtained only in an international terrorism case or a case that has an international terrorism nexus. 15 U.S.C. § 1681v. When information is obtained from a credit reporting company in response to a section § 1681u NSL, the requesting agent must review the information to assure that the credit reporting company did not provide a full credit report. If it did, the agent must redact any overproduced information.

NSL CREATED OUTSIDE FISAMS (Model ECs and NSLs)

(U//FOUO) NSLs should be created in FISAMS. If you have a reason to create an NSL outside the FISAMS subsystem (see DIOG 18.6.6.3.7), then you must use the Model ECs and NSLs (below), and the Deputy General Counsel of NSLB must approve the EC. Before you create an NSL outside FISAMS, read the "Guidance for NSLs Created Outside FISAMS" (under "FBI Resources" on the right-hand column).

1. Electronic Communications Privacy Act (ECPA) E-mail Subscriber EC
2. ECPA E-mail Subscriber NSL
3. ECPA E-mail Transactional EC
4. ECPA E-mail Transactional NSL
5. ECPA Telephone Subscriber EC
6. ECPA Telephone Subscriber NSL
7. ECPA Telephone Toll Billing Record EC
8. ECPA Telephone Toll Billing Record NSL
9. Fair Credit Reporting Act (FCRA) (a & b) (identity of financial institutions and consumer identifying information) EC
10. FCRA (a & b) (identity of financial institutions and consumer identifying information) NSL
11. 11. FCRA (a) (identity of financial institutions) EC
12. FCRA (a) (identity of financial institutions) NSL
13. FCRA (b) (consumer identifying information) EC
14. FCRA (b) (consumer identifying information) NSL
15. FCRA Full Credit EC
16. FCRA Full Credit NSL
17. Right to Financial Privacy Act (RFPA) (financial records) EC
18. RFPA (financial records) NSL
19. RFPA (correspondent account) EC
20. RFPA (correspondent account) NSL

LEGAL STANDARD: "RELEVANCE"

(U//FOUO) The legal standard for issuing an NSL is "relevance" to an authorized investigation to protect against international terrorism or clandestine intelligence activities. An investigation of a United States person

(USPER) cannot be conducted solely on the basis of activities protected by the First Amendment of the Constitution. An NSL may be issued in a preliminary or full investigation. The target of the NSL does not need to be the subject of the investigation. NSLB has created a training module on Virtual Academy that discusses all aspects of NSLs. You are encouraged to take the course if you have not done so recently. Search for the term "National Security Letters v2" in Virtual Academy.

APPROVAL AUTHORITY

(U//FOUO) A request for an NSL has two parts. First is the NSL itself, and the second is the EC approving issuance of the NSL, both of which are discussed below. The Director has delegated the authority to sign NSLs and to certify the nondisclosure requirement to the following FBI officials:

- Deputy Director
- Executive Assistant Director
- Assistant EAD for the National Security Branch
- Assistant Directors and all DADs for CT, CI, CyD, and the Weapons of Mass Destruction Directorate
- General Counsel
- Deputy General Counsel for the National Security Law Branch
- Assistant Directors in Charge in NY, LA, and D.C.
- All SACs

(U//FOUO) A copy of the signed NSL must be retained in the investigative case file and uploaded under the appropriate NSL document type in Sentinel. See EC dated 3/9/07 for more details on the NSL document type.

THE NSL

(U//FOUO) All NSLs must be addressed to the specific point of contact, which are listed in FISAMS. All NSLs should identify the statutory authority for the request, the type of records requested, and provide identifying information to assist the recipient in processing the request.

(U//FOUO) All NSLs require a certification that the records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities and that an investigation of a United States person is not conducted solely on the basis of First Amendment rights. The certification for a section 1681v NSL certification is slightly different to reflect its application to only international terrorism investigations.

(U//FOUO) The recipient of an NSL is informed of his right to challenge the nondisclosure provision as well as the NSL itself if compliance would be unreasonable, oppressive, or otherwise unlawful. The recipient is also informed that he may return the information to the FBI via federal express, secure fax, or personal delivery but not via regular mail or non-secure fax.

THE COVER EC

(U//FOUO) The cover EC serves five functions.

1. It documents the predication for the underlying investigation and that the information sought is relevant to an authorized investigation.
2. It documents the approval of the NSL by appropriate personnel.
3. It documents certification of the necessity for nondisclosure if one is included.
4. It contains information needed to fulfill Congressional reporting requirements for each type of NSL (subject's USPER status, type of NSL issued, and the number of phone numbers, e-mail addresses, account numbers, or individual records being requested in the NSL).
5. If the NSL is created outside FISAMS, the EC transmits information needed to fulfill Congressional reporting requirements to NSLB and to CTD, CD, CyD, or WMDD for informational purposes, and, in the case of personal service, to the appropriate field division for delivery of the NSL.

(U//FOUO) The EC must reference an investigative case file -- not a control file -- for which the information is sought. See EC dated 2/23/2007. The EC must set a lead to NSLB for informational and reporting purposes and a lead to the relevant HQ operational unit (CTD, CD, CyD, or WMDD) for informational purposes. There is no need to send a hard copy of the EC or NSL to NSLB or the relevant HQ operational unit.

INCLUDING A NONDISCLOSURE REQUIREMENT IN AN NSL

(U//FOUO) If nondisclosure of the NSL is sought, the EC must set forth the factual predicate for imposing nondisclosure. The certification supporting a nondisclosure obligation must assert that disclosure may endanger national security, interfere with a criminal, counterterrorism, or counterintelligence investigation; interfere with diplomatic relations; or endanger the life or safety of any person. Accordingly, the EC must establish why any of those dangers may arise from disclosure of the NSL. Possibilities include:

(U//FOUO) Disclosure may prematurely disclose a national security investigation to the subject of the investigation and thereby cause him or her to change his or her behavior to thwart detection.

(U//FOUO) Disclosure may prematurely disclose a national security investigation to the target of the NSL and thereby cause him or her to change his or her behavior to thwart detection or cause him or her to alert the subject of the investigation.

(U//FOUO) Disclosure may prematurely disclose a national security investigation to individuals who work with or are affiliated with the subject of the investigation, the target of the NSL, or the subject matter of the national security investigation and thereby cause those individuals to change their behavior to thwart detection or cause them to alert either the subject of the investigation or the target of the NSL.

(U//FOUO) Disclosure may alert other individuals engaged in international terrorism or clandestine intelligence activities who use the services of the NSL recipient from which the FBI asks for information and thereby cause those individuals to change their behavior to thwart detection.

(U//FOUO) Disclosure may persuade those engaged in international terrorism or clandestine intelligence activities to avoid patronizing the entity known to be the recipient of requests to provide information to the FBI and thereby allow those persons to thwart detection.

(U//FOUO) Disclosure may prematurely disclose a national security investigation and thereby cause surveillance techniques to be compromised or result in a danger to undercover FBI employees and confidential sources.

(U//FOUO) Disclosure may prematurely disclose a national security investigation and thereby provide an opportunity for someone to create intentionally flawed (i.e., compromised) foreign intelligence.

(U//FOUO) Disclosure may prematurely disclose a national security investigation involving a hostage situation and thereby result in a danger to the life or physical safety of a hostage or FBI employees trying to rescue the hostage.

(U//FOUO) Disclosure may prematurely disclose a national security investigation and thereby and thereby cause the subject of the investigation or a material witness to flee or to destroy or tamper with evidence.

(U//FOUO) Disclosure may prematurely disclose a national security investigation and thereby result in publicity that makes it difficult for the subject of the investigation or others to receive a fair trial.

(U//FOUO) Disclosure may prematurely disclose a national security investigation involving an imminent threat to terrorism and thereby result in a danger to the life or physical safety of others.

(U//FOUO) Disclosure may reveal the existence of a national security investigation involving a foreign government and thereby damage diplomatic relations.

(U//FOUO) This list is not exhaustive. There may be other reasons why an NSL should not be disclosed, and if so, those reasons should be set forth in the EC.

APPROVAL STANDARD FOR NSLs

(U//FOUO) NSLs created in a field office are reviewed by CDCs, while NSLs created at FBIHQ are reviewed by NSLB. NSLs must meet the legal standards set forth above, namely the information sought must be relevant to an authorized national security investigation. The EC must contain within its four corners sufficient information to allow a reviewer to determine the information sought is relevant to an authorized national security investigation.

(U//FOUO) The legal review conducted by the CDC is similar to the factual review the SAC conducts when certifying that the NSL is relevant to an authorized national security investigation and that the investigation is not based solely on the exercise of First Amendment rights by a USPER. An SAC cannot conduct the final review and approve the NSL when presented only with barebones information of the existence of an investigation and, for example, the target's telephone number or bank account number. A concise recitation of facts that supports the initiation and the continuation of the investigation is necessary for the SAC to conduct the final review and then approve the NSL.

NO EXIGENT LETTERS

(U//FOUO) The practice of using exigent letters to obtain NSL-type information is prohibited. See EC dated 3/1/2007, 319X-

HQ-A1487720-OGC, Serial 331. Instead, a Voluntary Emergency Disclosure Form (FD-1053) issued under 18 U.S.C. § 2702 should be used. FD-1053 describes the circumstances of the emergency and requests that the recipient make a determination that "an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." 18 U.S.C. § 2702(b)(8) and (c)(4). The disclosure does not need to be followed by legal process, although some recipients may ask that legal process be served on them in the future before they will release the information.

REPORTING REQUIREMENTS

(U//FOUO) NSLB is required to report information about NSL usage to Congress. It is crucial that the portion of the EC that addresses reporting requirements is accurate. While an EC may cover more than one target, more than one account, and even more than one recipient, the EC must delineate the number of targeted phone numbers, e-mail accounts, financial accounts, and/or credit agency reports that are issued to each NSL recipient. For example, if there are three targets and five e-mail accounts, and two service providers who will be the recipients of the NSL, then the EC must state how many accounts are associated with the NSL issued to each recipient. It is not sufficient to list in the EC that there are five e-mail accounts and two recipients. FISAMS automatically tallies statistics needed for congressional reporting, so drafters and reviewers should verify that the statistics are accurately reported in FISAMS and the same is accurately reflected in the EC.

(U//FOUO) The FBI must also report to congress the USPER status of the target of the NSL (as opposed to the subject of the investigation). While the subject of the investigation is often the target of the NSL, sometimes that is not the case. Therefore, the EC must memorialize the USPER status of the target of the NSL, i.e., the person whose information the FBI is obtaining. If the FBI is obtaining information about more than one person, the EC must reflect the USPER status of each person.

DISSEMINATION OF NSL MATERIAL

(U//FOUO) Information obtained using an NSL may be disseminated in accordance with general standards set forth in the Attorney General Guidelines for Domestic FBI Operations (AGG-Dom). Dissemination is further subject to specific statutory limitations. For example, ECPA, 18 U.S.C. § 2709, and RFPA, 12 U.S.C. § 3414(a)(5)(B), permit dissemination if the information is clearly relevant to responsibilities of the recipient agency. FCRA, 15 U.S.C. § 1681u, permits dissemination to other federal agencies as may be necessary for the approval or conduct of a counterintelligence investigation.

RETAINING NSL INFORMATION

(U//FOUO) All responsive records remain with the investigative file until the file is destroyed in accordance with the National Archives and Records Administration.

REVIEW OF AN NSL NONDISCLOSURE REQUIREMENT

(U//FOUO) The USA FREEDOM Act of 2015 requires the FBI to review at certain intervals during the investigation all National Security Letters (NSL) that included a nondisclosure requirement pursuant to procedures adopted by the Attorney General. Pursuant to the *Attorney General Termination Procedures for National Security Letter Nondisclosure Requirement (Procedures)*, issued November 24, 2015, the review is to determine whether the nondisclosure requirement in an NSL should continue or be terminated. Under these *Procedures*, the nondisclosure requirement of an NSL shall terminate upon the closing of any investigation in which an NSL containing a nondisclosure provision was issued except where the FBI makes a determination that one of the existing statutory standards for nondisclosure is satisfied. Pursuant to the *Procedures*, starting February 21, 2016, when (i) an open investigative file reaches its third-year anniversary (i.e., three years from the Sentinel case opening date) and (ii) an investigative file is closed, an NSL nondisclosure review must occur. If an investigation is closed before its third-year anniversary, then the NSL nondisclosure review will occur once, that is, when the investigation closes. There are no NSL nondisclosure reviews beyond the third-year anniversary and/or when the investigative file is closed.

(U//FOUO) Sentinel identifies when an NSL nondisclosure review must occur. On a daily basis, Sentinel searches for any investigative file that has reached its third-year anniversary or was closed. Sentinel then automatically sets a lead to the current supervisor of the "Owning Squad" from which the NSL was issued. The supervisor may complete the review or reassign the lead to the agent identified as the "Primary Case Manager" or to another person, such as another case manager or a case participant. The Sentinel generated lead should be covered only after each NSL issued in the investigative file has been reviewed and an individual determination is made whether the nondisclosure requirement should continue or be terminated. The NSL nondisclosure review must be documented in the FISA Management System (FISAMS) in the same FISAMS workflow assigned to the NSL.

(U//FOUO) The NSL nondisclosure review consists of the case agent assigned to the investigation reviewing the NSL and the basis for initially including a nondisclosure requirement. The case agent then assesses whether the nondisclosure requirement should continue or may be terminated based on the current facts and circumstances surrounding the investigation. DIOG Section

18.6.6.3.7.1 lists several potential reasons why the nondisclosure requirement should possibly continue. The list is not exhaustive, so if there are other reasons that explain why an NSL nondisclosure requirement should continue, the EC should explain those reasons. The presumption is that the NSL nondisclosure requirement will be terminated unless there is an articulable basis to continue it. After the case agent has made the determination to continue or terminate NSL nondisclosure requirement and created the EC in FISAMS memorializing the determination, FISAMS will send the EC to the SSA, CDC, ASAC, and SAC for review and approval. If the SAC approves terminating the NSL nondisclosure requirement, FISAMS will create a letter for the SAC to sign and send to the NSL recipient announcing the FBI has terminated the NSL nondisclosure requirement.

(U//FOUO) The review of an NSL nondisclosure requirement should be completed within thirty (30) days of the lead assignment. The Sentinel generated lead should be covered only after the review of all the NSLs in the investigative file has been completed.

CLASSIFICATION OF EC AND NSL

(U//FOUO) Although the EC authorizing the NSL is classified because it discusses the underlying investigation, the NSL itself is not classified, nor is the material received in response to the NSL classified. Information obtained in response to an NSL may be used in criminal proceedings without declassification. However, if the information concerning the account number, telephone number, or subscriber used in an NSL was initially obtained through the results of a FISA, the DOJ's Office of Intelligence may consider the information to be FISA-derived and therefore needs Attorney General approval before using the NSL results in criminal proceedings.

POINT OF CONTACT FOR NSL RECIPIENTS

(U//FOUO) If you wish to update a point of contact (POC) for a particular recipient of NSLs, please visit the SharePoint site [redacted] complete the form, and then submit the form by clicking "Save." The FISA Unit will review your changes and incorporate them into FISAMS.

ADDITIONAL RESOURCES

1. EC dated 5/27/2005, 319X-HQ-A1487720-OGC, Serial 20, which authorizes the use of return dates.
2. EC dated 6/29/2005, 319X-HQ-A1487720-OGC, Serial 24, which relates to use of restricted delivery services to serve NSLs.
3. EC dated 3/20/2006, 319X-HQ-A1487720-OGC, Serial 213, which permits the FBI to serve NSLs by non-secure fax under certain conditions.
4. EC dated 4/11/2006, 319X-HQ-A1487720-OGC, Serial 222, which relates to the FBI's reimbursement policy for NSLs.
5. EC dated 4/4/2007, 319X-HQ-A1487720-OGC, Procedures for Redacting NSL Results.
6. EC dated 11/30/2007, 319W-HQ-A1487699-OGC, Serial 24, which relates to the creation of the NSL subsystem in FISAMS.
7. EC dated 6/1/07, 319X-HQ-A1487720, which provides guidance on the use, requirement, and reporting of NSLs.